

Sources, Limitations and Conditions for Testing

Supporting document for the parent-led AI Learning Framework for ages 13-16.

Operating model

Parent leads. Learner engages. AI supports.
The framework supports a family learning arrangement. It does not replace a parent, teacher, school, therapist, safeguarding service or emergency service.

England context | UK data-protection and provider rules | Version 1.2

Operating position

This is an experimental, parent-led learning framework. It is not a legally enforced system, technical lock, safeguarding service or substitute for parenting, teaching, professional support or emergency action.

How these sources should be read

The documents below do not all impose duties on a parent using an AI service at home. Some govern schools, colleges, public bodies, technology suppliers or organisations processing children's data. They are included because their principles inform a cautious design.

Source type	Role in this framework
Law and data-protection regulation	May apply to organisations processing personal data or operating a service; applicability depends on the real operating model.
School statutory guidance	Directly relevant to schools and colleges. It informs but does not certify private family use.
DfE product and education guidance	Informs safety, human oversight, transparency and risk assessment.
Provider terms	Govern the selected service's minimum age, permission, account and acceptable-use rules.
Pedagogical design	Framework choices such as scaffolding, guided practice and another attempt before correction; not presented as legal duties.

1. Current authority and timing

Source	Current position at 2 August 2026
Keeping Children Safe in Education	KCSIE 2025 remains operative until 31 August 2026. KCSIE 2026 has been published and takes effect on 1 September 2026. It applies to schools and colleges.
Working Together to Safeguard Children	The 2026 statutory guidance applies in England to relevant organisations and practitioners working to safeguard children.
DfE generative AI product safety standards	Updated 19 January 2026 to include cognitive, emotional and social development, mental health and manipulation.
ICO Children's Code and UK GDPR guidance	Relevant where an online service processes children's personal data; emphasises best interests, high privacy and data minimisation.
Provider rules	Must be checked for the selected service. For ChatGPT, users aged 13-17 require parent or guardian permission and account credentials must not be shared.

2. How the framework applies the principles

Framework rule	Reason for inclusion
Parent remains responsible	Human oversight and the framework's non-enforcement limitation.
Learner knows reviews occur	Trust, transparency and protection against covert monitoring.
Prompt rules are not security	General-purpose AI may ignore, misunderstand or inconsistently apply instructions.
No account sharing	Provider terms and basic account security.
Minimal personal information	Data minimisation and child-centred privacy.
No diagnosis, therapy or grading	Professional boundaries, accuracy and fairness.
Pause serious disclosures	Safeguarding principle: stop learning and involve real people rather than investigate.
No alerting claim	The AI cannot guarantee memory, notify a parent or replace supervision.
Scaffold before answer	Pedagogical design supporting reasoning and another attempt.

3. Main authoritative sources

Keeping Children Safe in Education 2025 and 2026

School safeguarding duties, online safety, filtering, monitoring and professional responsibilities.

gov.uk/government/publications/keeping-children-safe-in-education--2

Working Together to Safeguard Children 2026

Multi-agency safeguarding guidance and proportionate information sharing in England.

gov.uk/government/publications/working-together-to-safeguard-children--2

DfE Generative AI Product Safety Standards

Age appropriateness, transparency, harmful-content controls, monitoring, cognitive and emotional development and manipulation risks.

gov.uk/government/publications/generative-ai-product-safety-standards

DfE Generative Artificial Intelligence in Education

Risk assessment, human oversight, data protection, inaccuracy, bias and safe educational use.

gov.uk/government/publications/generative-artificial-intelligence-in-education

DfE Safe Use of Generative AI in Education - Module 3

Safeguarding, ethics, data and intellectual-property risks; updated for 2026-27.

gov.uk/government/publications/safe-use-of-generative-ai-in-education-module-3

ICO Children's Code and children and UK GDPR

Best interests, high privacy by default, data minimisation and child-appropriate information.

ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/

Data (Use and Access) Act 2025

Amends and builds on the UK GDPR and Data Protection Act 2018. Applicability depends on the operating and data-processing model.

gov.uk/guidance/data-protection-in-schools/the-data-use-and-access-act-2025

OpenAI UK/EEA terms and age guidance - provider example, not endorsement

Minimum age 13, parental permission for under-18s and no sharing of account credentials. Other providers must be checked separately.

openai.com/policies/eu-terms-of-use/

help.openai.com/en/articles/8313401-is-chatgpt-safe-for-all-ages

Childline

UK support for children and young people. Free telephone support on 0800 1111; emergencies require 999.

childline.org.uk/get-support/contacting-childline/

4. Conditions for parent-led testing

Condition	Required position
Purpose	Supports parent-led learning; not a teacher, therapist, safeguarding service, emergency service or technical control.
Agreement	Parent and learner agree the purpose, boundaries and review arrangement before use.
Age and account	Learner meets provider age rules, has required permission and does not use shared credentials.
Prompt limitations	Rules may be ignored, bypassed or applied inconsistently.
Review scope	PARENT REVIEW summarises only content still available in the same conversation.
No authentication	The phrase does not verify that the requester is the parent.
No monitoring or alerts	The AI does not guarantee a hidden record or contact a parent, school or emergency service.
Privacy	Avoid unnecessary identifying, school, contact, family, health and safeguarding information.
Safeguarding	Serious disclosures stop learning and are directed to a trusted adult; the AI does not investigate.
Academic integrity	The framework supports learning but not dishonest completion of assessed work.
Accuracy	AI output may be wrong. Important information must be checked.
No certification	Not government endorsed, legally approved or independently certified.
Review	Sources and conditions must be updated when law, guidance or platform terms change.

5. Data and publication conditions

The downloadable framework itself does not need to collect personal data. A future Post-Social setup tool should generate the prompt in the browser without transmitting or storing the family's selections.

- Do not ask for the learner's name, school, contact details or personal profile in the setup tool.
- Explain that the selected AI provider, not Post-Social, processes the conversation under its own terms and privacy policy.
- Do not claim that the parent review creates a private or secure parent channel.
- Do not store generated prompts or choices unless a separate, reviewed privacy model is introduced.
- Publish a visible correction date and version number because provider terms and guidance change.

6. Before any public trial

- Test the prompt on the intended AI services and account types.
- Test context loss, separate-chat failure and attempts by a learner to invoke PARENT REVIEW.
- Test unsafe output, dependency language, disclosures, bias, SEND accessibility, visual accessibility and academic integrity.
- Test that hints and visuals do not accidentally reveal answers or introduce misconceptions.
- Publish incident, correction, deletion and complaint routes for the framework webpage.

7. Before any school pilot

- Obtain designated safeguarding lead review and institutional approval.
- Complete legal and data-protection review of the actual operating model.
- Complete a DPIA and privacy notice where children's personal data is processed.
- Complete platform, procurement, filtering, monitoring and accessibility checks.
- Document safeguarding, complaints, incident, correction, deletion and escalation procedures.

Status

Suitable as a supporting evidence and limitations document for controlled parent-led testing. It does not establish legal compliance or safeguarding certification.